Proposition de recherche doctorale

SECURISATION D'UN PROCESSEURS VIS-A-VIS DES ATTAQUES EN FAUTE ET PAR ANALYSE DE LA CONSOMMATION

Mots clés :

- **Directeur de thèse** : Nathalie Drach-Temam
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire d'informatique de Paris 6
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Les circuits intégrés de sécurité comme ceux qui sont utilisés dans les cartes à puce, parce qu'ils contiennent des informations confidentielles, font l'objet de manipulations frauduleuses, appelées communément attaques, de la part de personnes mal intentionnées. Plusieurs attaques ont été répertoriées et analysées. Les plus efficaces d'entre-elles consistent à mesurer la consommation du circuit lorsque celui-ci réalise des calculs cryptographiques ou à altérer son fonctionnement (notamment grâce à un laser) puis à utiliser des outils mathématiques permettant d'extraire les informations sensibles de ces mesures. Le travail de thèse porte sur la protection d'un microprocesseur embarqué dans les circuits de sécurité tels que la carte-à-puce contre les attaques répertoriées avec une attention particulière portée aux attaques en faute. L'approche consistera à intégrer des spécifications sécuritaires dans les modèles architecturaux de processeurs puis de créer ou d'adapter des outils de génération automatique afin d'obtenir des modèles matériels vérifiant ces spécifications. Dans un premier temps, il s'agit de faire l'état de l'art des attaques ainsi que les contre-mesures proposées dans la littérature (masquage de l'information sensible par des aléas, redondance des données, équilibrage des chemins de propagation etc...) Dans un second temps, les contre-mesures, proposées dans le cadre de thèse, seront implantées et validées sur un processeur expérimental. Le résultat obtenu de solutions proposées doivent offrir un faible surcoût en terme de matériel et de performance.